CLAIMS:

1. A method of authenticating a mobile node to a communication system, the communication system comprising a plurality of access nodes, the method comprising:

(a) generating a numerical chain comprising a series of values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value;

(b) sending a value from the first numerical chain from the mobile node to an access node to which the mobile node wishes to attach; and

(c) using the sent value at the access node to authenticate the mobile node.

2. A method according to claim 1, wherein an authenticating node is provided with values of the first numerical chain earlier in the sequence than the sent value, the authenticating node authenticating the mobile node on the basis of a comparison of the output of the one-way coding function when applied to the sent value, and an earlier value of the first numerical chain.

3. A method according to claim 2, wherein the comparison of the sent value and an earlier value of the first numerical chain comprises comparing the output of the one-way coding function applied at least once to the sent value to an earlier value of the first numerical chain.

4. A method according to any preceding claim, wherein the earlier value of the first numerical chain is the value immediately preceding the sent value.

5. A method according to any one of claims 2 to 4, wherein the authenticating node is the access node to which the mobile node wishes to attach.

6. A method according to claim 5, wherein the authenticating node sends a notification update to the remainder of the plurality of access nodes upon successful authentication of the mobile node.

7. A method according to claim 6, wherein the update notification is issued through a secure local multicast mechanism.

8. A method according to any one of claims 2 to 4, wherein the authenticating node is a control node which communicates with the plurality of access nodes.

9. A method according to claim 8, wherein the authenticating node stores an update notification upon successful authentication of the mobile node.

10. A method according to claim 6 or 9, wherein the notification update comprises the sent value provided by the mobile node.

11. A method according to any preceding claim, wherein a value H_{i-1} of the first numerical chain may be obtained from a value H_i of the first numerical chain using the one-way coding function defined such that $H_{i-1} = \mathtt{hash}(H_i)$.

12. A method according to any preceding claim, wherein the first numerical chain is generated by providing a seed value H_n of the numerical chain, all preceding values being obtainable through successive application of the one-way coding function.

13. A method according to claim 12, wherein the seed value H_n is based upon a value known only to the mobile node and a home network.

14. A method according to claim 12, wherein the seed value H_n is based upon a value known only to the mobile node.

15. A method according to any one of claims 12 to 14, wherein the seed value H_n is based upon the EAP MSK or EMSK value.

16. A method according to any one of claims 12 to 14, wherein the seed value H_n is based upon a randomly generated value.

17. A method according to any one of claims 12 to 16, wherein the seed value is encrypted so that the access nodes cannot determine the seed value.

18. A method according to any one of claims 2 to 17, wherein the first value of the numerical chain, obtained from successive applications of the one-way coding function to a seed value, is provided to the authenticating node by either the mobile node or a home network to which the mobile node is subscribed.

19. A method of authenticating a mobile node to a communication system, the communication system comprising a plurality of access nodes and a plurality of interfaces, the method comprising generating a plurality of numerical chains, each of the plurality of numerical chains corresponding to one of the plurality of interfaces, and authenticating the mobile node on a plurality of the interfaces in accordance with the method of claim 1.

20. A method according to claim 19, wherein the mobile node authenticates itself to the plurality of interfaces in parallel.

21. A method according to any preceding claim, wherein a value of the numerical chain is used to generate at least part of an IP address for the mobile node.

22. A method according to any preceding claim, wherein each numerical chain is bound to a specific MAC address corresponding to a specific access node.

23. A method according to any preceding claim, wherein the communication system comprises a wireless access network, and the mobile node is a wireless terminal.

24. A method of authenticating a mobile node when roaming within a communication system, the method comprising:

following handover of the mobile node from a first access node of the communication system to a second access node, authenticating the mobile node to the second access node using the method of any one of the preceding claims.

25. A method according to claim 25, wherein the mobile node has been previously authenticated to the said communication system by a home network of the mobile node.

26. A method of deriving a secure authentication key when a mobile node authenticates itself to an access node in accordance with any preceding claim, the method comprising:

providing a first authentication key K_{S0} for use by the mobile node and a first access node;

sending a hash of the first authentication key $\texttt{hash}(K_{S0})$ to a second access node and the mobile node; and

generating a new authentication key K_{S1} in accordance with the hash $\texttt{hash}(K_{S0})$.

27. A method according to claim 26, wherein the new authentication key is generated by taking a hash of the hash $\texttt{hash}(K_{S0})$, in accordance with the function $K_{S1} = \texttt{hash}(\texttt{hash}(K_{S0}))$.

28. A method according to claim 26, further comprising the steps of:

exchanging a first nonce N_{C1} provided by the mobile node and a second nonce N_{A1} provided by the second access node between the mobile node and the second access node; and wherein the new authentication key K_{S1} is generated in accordance with the hash of the first session key K_{S0}, the first nonce N_{C1} and the second nonce N_{A1} in accordance with the function $K_{S1} = \texttt{hash}(\texttt{hash}(K_{S0}), N_{C1}, N_{A1})$.

29. A mobile wireless terminal, the terminal comprising means for generating and storing a first numerical chain comprising a series of n values using a one-way coding

function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value; and means for disclosing values from the numerical chain to an access node in order to allow the access node to authenticate the mobile wireless terminal.

30. An access node of a communication system having means for receiving from a mobile node a value of a first numerical chain comprising a series of *n* values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value; and means for authenticating the mobile node on the basis of that value.

31. A control node of a communication system having means for receiving from a mobile node or an access node a value of a first numerical chain comprising a series of *n* values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value; and means for authenticating the mobile node on the basis of that value.